REMARKS

The Office Action mailed December 31, 2007 has been carefully considered. Reconsideration in view of the following remarks is respectfully requested.

Record of Interview

On April 2, 2008, an interview was conducted by telephone between Examiner Shanto Abedin and the undersigned. The Applicants thank the Examiner for granting this interview. The details of the interview are set forth in the Interview Summary document made of record.

Claim Status and Amendment of the Claims

Claims 1-46 are currently pending.

No claims stand allowed.

Claims 1-46 have been amended to further particularly point out and distinctly claim subject matter regarded as the invention. Specifically, all occurrences of "said" have been replaced with "the." Support for these changes may be found in the specification, figures, and claims as originally filed.

The First 35 U.S.C. § 103 Rejection

Claims 1-3, 6-7, 11, 13-15, 17, 23-25, 28-29 and 44-46 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Kanuri et al.[1] in view of Short et al.,[2] among which claims 1, 13, and 23 are independent claims.[3] This rejection is respectfully traversed.

[1] U.S. Patent No. 6,807,179 to Kanuri et al.
[2] U.S. Patent No. 7,194,554 to Short et al.
[3] Office Action mailed December 31, 2007, ¶ 5.

According to the Manual of Patent Examining Procedure (M.P.E.P.),

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in the applicant's disclosure.[4]

Claim 1

Claim 1 as presently amended recites:

> A layer 2 network access device for providing network security, comprising: a plurality of input ports;
> a switching fabric in the layer 2 network access device for routing data received on the plurality of input ports to at least one output port; and
> control logic in the layer 2 network access device adapted to authenticate a physical address of a user device coupled to one of the plurality of input ports, to authenticate user information provided by a user of the user device only if the physical address is valid, and to restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information only if the user information is valid.

The Examiner states,

> ... Kanuri et al teaches a layer 2 network access device for providingnetwork security, comprising:
> a plurality of input ports (Fig 1, 12.22; Col 3, lines 25-67; multiport switch)
> a switching fabric in the layer 2 network access device for routing data received on saidplurality of input ports to at least one output port (Fig 1.28; Col 3, lines 25-67; switch fabric; Col 4,lines 7-52; layer 2 switch); and
> control logic in the layer 2 network access device (Col 3, line 28 to Col 5, line 65: the switch; MAC module; switching (rules) logic) adapted to authenticate a physical address of a user device coupled to one of said plurality of input ports (Col 3, line 28 to Col 5, line 65; matching MAC addresses), to authenticate user information provided by a user of said user device only if said physical address is valid (Col 3, line 54 to Col 4, line 34; Col 5, lines 10-65; user, or network nodes' attributes/ policies/ information; user defined policies/ attributes; authenticating VLAN field/ index/ information, and MAC addresses specific to user/ network node/ data frame), and to restrict access to said one of said plurality of input ports in accordance with a user policy associated with said user information only if said user information is valid (Fig 2:40; associated port, MAC and VLAN information;

[4] M.P.E.P § 2143.

> Fig 3, step 70-106; Col 5, lines 43-60; if in step 74 the switching rules logic determined a match between MAC...VLAN index .... (then) checks in step 76 whether port ...; the examiner interprets switching "rules" logic as policy; port filtering).
> In the case, obviousness regarding authenticating user provided authentication information, and MAC is not found to be supportive, the examiner notes, Short et al discloses network security/ access device authenticating user provided authentication information, and MAC (Fig 2; Col 4, starts at line 12; authentication; user id; MAC). Short et al and Kanuri et al are analogous art because they are from the same field of endeavor of secure network communication. At the time of invention, it will be obvious to a person of ordinary skill in the art to combine the teachings of Short et al with Kanuri to design an apparatus wherein network security/ access device authenticates user provided authentication information, and MAC in order to provide further security to the system.[5]

The Applicants respectfully disagree for the reasons set forth below.

Kanuri et al. In View Of Short et al. Does Not Disclose To Authenticate User Information Provided By A User Of The User Device Only If The Physical Address Is Valid, And To Restrict Access To The One Of The Plurality Of Input Ports In Accordance With A User Policy Associated With The User Information Only If The User Information Is Valid

In support of the Examiner's contention that Kanuri et al. in view of Short et al. discloses authenticating user information provided by a user of the user device only if the physical address is valid, the Examiner refers to the following portion of Kanuri et al.:

> The switch 12 includes network switch ports 22, and a switch fabric 28. Each network switch port 22 includes a media access control (MAC) module 24 that transmits and receives layer 2 type data packets to the associated network stations 14 or 16, and port filters 26. Each port filter 26, also referred to as a packet classifier, is configured for identifying a user-selected attribute of the layer 2 type data frame, described below, and outputting the relevant switching information (e.g., whether the user-selected attribute was detected) to the switch fabric 28. As described below, the switch fabric 28 is configured for making trunk-based layer 2 switching decisions for received layer 2 type data packets.
>
> As shown in FIG. 1, the switch 12 has an associated host CPU 30 and a buffer memory 32, for example an SSRAM. The host CPU 30 controls the overall operations of the corresponding switch 12, including programming of the port filters 26 and the switch fabric 28. The buffer memory 32 is used by the corresponding switch 12 to store layer 2 type data frames while the switch fabric 28 is processing forwarding decisions for the received layer 2 type data packets.

[5] Office Action dated December 31, 2008, pp. 3-4.

> The switch fabric 28 is configured for performing layer 2 switching decisions and switching decisions that implement user-defined switching policies; such user-defined switching policies may include supporting trunk-based traffic having a prescribed user-selected attribute, for example having been determined to belong to a prescribed flow, for example an IGMP media flow or other flow having a prescribed TCP source address and/port TCP destination address, or granting sufficient switch resources to ensure a guaranteed quality of service (e.g., reserved bandwidth or guaranteed latency).
>
> According to the disclosed embodiment, each port filter 26 of FIG. 1 is configured for identifying user-selected attributes, from a received layer 2 type data frame, that are used by the switching logic 28 to perform trunk-based switching decisions. The port filter 26 can be implemented as a state machine that monitors the bytes coming in from the network, hence the state machine can analyze the layer 2 type data frame for the presence of prescribed user-selected attributes (e.g., TCP source port and/or TCP destination port) on a per-byte basis as the bytes of packet data of the data frame are received by the network switch port. In addition, the port filter 26 can be configured for multiple simultaneous comparisons of the incoming packet data with multiple templates that specify respective user-selected attributes, enabling the port filter 26 to simultaneously determine the presence of a plurality of user-selected attributes as the layer 2 type data frame is received.[6]

The above disclosure of Kanuri et al. speaks generally about performing layer 2 switching decisions that implement user-*defined* switching policies. Examples of such user-defined switching policies "include supporting trunk-based traffic having a prescribed user-selected attribute, for example having been determined to belong to a prescribed flow, for example an IGMP media flow or other flow having a prescribed TCP source address and/port TCP destination address, or granting sufficient switch resources to ensure a guaranteed quality of service (e.g., reserved bandwidth or guaranteed latency)."[7] But nowhere does the cited portion of Kanuri et al. disclose authenticating *user* information *provided* by a user of the user device, let alone authenticating user information provided by a user of the user device only if the physical address is valid as required by Claim 1. The Examiner has not identified in Kanuri et al. user information provided by the user of the user device. The Applicants respectfully submit the

[6] Kanuri et al. at col. 3 l. 54 to col. 4 l. 54.
[7] Kanuri et al. at col. 4 ll. 10-16.

Examiner's attempt to equate authenticating user information provided by a user of a user device with merely identifying the presence of user-selected attributes in a received layer 2 type data frame is improper.

The Examiner also refers to the following portion of Kanuri et al. in support of the Examiner's contention that Kanuri et al. discloses authenticating user information provided by a user of the user device only if the physical address is valid:

> Hence, the switching rules logic 42 can determine which trunk a port belongs to by accessing the trunk table by the corresponding port number.
> The trunk distribution table 48 is a thirty-two row by eight column wide table configured for storing, for each of eight identified trunk fields 60, the switch ports 22 that serve the corresponding identified trunk 20. As illustrated in FIG. 2, switch ports 1-4 are assigned to "Trunk1" specified in trunk field 60.sub.1, switch ports 5-8 are assigned to "Trunk2" specified in trunk field 60.sub.2, switch ports 5-8 are assigned to "Trunk3" specified in trunk field 60.sub.3, etc. In addition, the assigned ports are stored by the host CPU 30 as a prescribed repeating sequence within the corresponding column 60 of the trunk distribution table 48, enabling the switching rules logic 42 to select any one of the ports 22 associated with a given trunk field 60 by generating a hash key index value 62 in the hash key generator 46 based on selected attributes within the received layer 2 type data frame, for example MAC source address, MAC destination address, TCP source port, and/or TCP destination port. Hence, the switching rules logic 42 accesses the trunk distribution table 48 by first determining a destination switch port from the address table 40. Upon determining the destination switch port from the port vector field 58 corresponding to a matched destination MAC address 52 or a VLAN field 56, the switching rules logic 42 determines the corresponding served trunk from the trunk table 44. Upon determining the output trunk from the trunk table 44, the switching rules logic 42 accesses the column for the identified output trunk 60 in the trunk distribution table 48, and accesses one of the rows of the table 48 based on the corresponding hash key index value 62 generated by the hash key generator 46.
> FIG. 3 is a diagram illustrating the method generating trunk-based switching decisions by the switch fabric 28 according to an embodiment of the present invention. The method begins by the switching rules logic 42 receiving, from the switch port 22, layer 2 header information for the received data packet (including MAC source address, MAC destination address, VLAN information), and an indication from the corresponding packet classifier module 26 whether the received data packet includes a prescribed pattern corresponding to a prescribed data flow (e.g., by identifying TCP source port and/or TCP destination port). As

> described above, the host CPU 30 may program the port filter 26 of each network switch port 22 to identify any one of a plurality of prescribed patterns, such that the port filter 26 may be able to distinguish between IGMP frames, SMTP frames, LDAP frames, etc., as well as identify prescribed data flows. Alternatively, the switching rules logic 42 may include a parsing engine to identify the MAC addresses and the TCP ports.
> The switching rules logic 42 performs an ingress check in step 70, for example by confirming according to prescribed ingress rules that the received data packet is a valid data frame. The switching rules logic 42 then searches the address table 40 in step 72 based on the source MAC address in the received data frame to confirm that the transmitting network node information is stored in the address table 40. If in step 74 the switching rules logic 42 determines a match between the source MAC address and/or the VLAN index with an address table entry 50, the switching rules logic 42 checks in step 76 whether the port field 54 matches the identifier of the switch port 22 having received the data packet; if there is no match, and if in step 78 the port does not belong to the same trunk, then the entry is overwritten in step 80, otherwise a hit bit is set in steps 82 or 84 to prevent subsequent deletion of the entry 50 by aging functions.
> If in step 74 there is no match of the source MAC address or the VLAN index with any entry in the address table 40, the switching rules logic 42 learns the new address in step 86 and stores the new address information as a new entry in the address table 40.[8]

The above disclosure of Kanuri et al. speaks generally about generating trunk-based switching decisions which include performing ingress checks on a received data packet based on a source MAC address. But nowhere does the cited portion of Kanuri et al. disclose authenticating user information provided by a user of the user device, let alone authenticating user information provided by a user of the user device only if the physical address is valid as required by Claim 1. Again, the Applicants respectfully submit the Examiner's attempt to equate authenticating user information provided by a user of a user device with merely identifying the presence of user-selected attributes in a received layer 2 type data frame is improper.

The Examiner also refers to the following portion of Short et al. in support of the

[8] Kanuri et al. at col. 5 ll. 10-65.

Examiner's contention that Short et al. discloses authenticating user information provided by a user of the user device only if the physical address is valid:

> In operation, a source computer requests (block 200) access to a network, destination, service, or the like. Upon receiving a packet transmitted to the AAA server 30, the AAA server 30 examines the packet to determine the identity of the source (block 210). The attributes transmitted via the packet are temporarily stored in the source profile database so that the data can be examined for use in determining authorization rights of the source. The attributes contained in the packet can include network information, source IP address, source port, link layer information, source MAC address, VLAN tag, circuit ID, destination IP address, destination port, protocol type, packet type, and the like. After this information is identified and stored, access requested from a source is matched against the authorization of that source (block 230).
>
> Once a source profile has been determined by accessing the authorization rights stored in the source profile database, three possible actions can result. Specifically, once a source's authorization rights have been retrieved the AAA server 30 may determine a source to have access 222, to be pending or in progress 224, or to not have access 226. First, a source is deemed valid (i.e., to have access) where the source profile database so states. If a source is determined to be valid, the source's traffic can be allowed to proceed out of the gateway device to the networks or online services the user associated with the source wishes to access (block 230). Alternatively, the source may be redirected to a portal page, as described in the Redirecting Application, prior to being allowed access to the requested network. For example, a user may be automatically forwarded to a user-input destination address, such as an Internet address, for example, where a user has free access associated with the user's hotel room. Alternatively, this may occur where the user has already purchased access and the user has not exhausted available access time. Furthermore, an accounting message may be initiated 230 to log the amount of time the user is utilizing the gateway device such that the user or location may be billed for access.
>
> If the second scenario occurs, in which the source is deemed pending 224 or in progress, the source may take steps to become authenticated (block 240) so that the source information is recorded in the source profile database. For example, a user may have to enter into a purchase agreement, requiring the user to enter a credit card number. If the user needs to purchase access, or if the system needs additional information about the user, the user can be redirected from the portal page via Home Page Redirect (HPR) and Stack Address Translation (SAT) to a location, such as a login page, established to validate new users. SAT and HPR can intervene to direct the user to a webserver (external or internal) where the user has to login and identify themselves. This process is described in detail in the Redirecting Application. After inputting any necessary and sufficient information, the user is then be permitted access to a destination address (block 230, 250). Where the information provided is insufficient the user will not be authorized access (block 260). Finally, a third scenario can occur in which a

> source is deemed not to have access 226 so that the user is not permitted to access a destination via the network (block 260).[9]

The above portion of Short et al. speaks generally about a distributed authentication solution whereby a AAA server is configured to determine authorization rights of a source computer requesting access to a network, and possibly *redirect* or *forward* the request to a portal page which will prompt a user for additional authentication.[10] Short et al. also speaks about further redirecting or forwarding the request from the portal page to yet *another* location to validate new users.[11] Whereas Claim 1 requires the claimed device comprise control logic to, *inter alia*, (1) authenticate a physical address of a user device coupled to one of the plurality of input ports, and (2) authenticate user information provided by a user of the user device only if the physical address is valid. For this additional reason, the 35 U.S.C. § 103 rejection of Claim 1 based on Kanuri et al. in view of Short et al. is unsupported by the cited art of record.

In support of the Examiner's contention that Kanuri et al. discloses to restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information only if the user information is valid, the Examiner refers to step 76 of FIG. 3. The corresponding disclosure in Kanuri et al. recites:

> The switching rules logic 42 performs an ingress check in step 70, for example by confirming according to prescribed ingress rules that the received data packet is a valid data frame. The switching rules logic 42 then searches the address table 40 in step 72 based on the source MAC address in the received data frame to confirm that the transmitting network node information is stored in the address table 40. If in step 74 the switching rules logic 42 determines a match between the source MAC address and/or the VLAN index with an address table entry 50, the switching rules logic 42 checks in step 76 whether the port field 54 matches the identifier of the switch port 22 having received the data packet; if there is no match, and if in step 78 the port does not belong to the same trunk, then the entry

[9] Short et al. at col. 12 l. 21 to col. 13 l. 14.
[10] Short et al. at col. 12 ll. 48-54.
[11] Short et al. at col. 12 l. 65 to col. 13 l. 3.

> is overwritten in step 80, otherwise a hit bit is set in steps 82 or 84 to prevent subsequent deletion of the entry 50 by aging functions.[12]

Nowhere does the portion of Kanuri et al. cited by the Examiner disclose restricting access to the one of the plurality of input ports in accordance with a user policy associated with the user information *only if the user information is valid.* The Applicants respectfully submit the Examiner's attempt to equate port filtering with restricting access to the one of the plurality of input ports in accordance with a user policy associated with the user information only if the user information is valid as required by Claim 1 is improper. For these reasons, the 35 U.S.C. § 102 Rejection of Claim 1 is unsupported by the cited art of record. Thus, a *prima facie* case has not been established and the rejection must be withdrawn.

Claims 13 and 23

Claim 13 is a method claim corresponding to apparatus claim 1. Claim 23 is a system claim corresponding to apparatus claim 1. Claim 1 being allowable, Claims 13 and 23 must be allowable for at least the same reasons as Claim 1.

Dependent Claims 2-3, 6-7, 11, 14-15, 17, 24-25, and 28-29

Claims 2-3, 6-7, and 11 depend from Claim 1. Claims 14-15 and 17 depend from Claim 13. Claims 24-25 and 28-29 depend from Claim 23. Claims 1, 13, and 23 being allowable, Claims 2-3, 6-7, 11, 14-15, 17, 24-25, and 28-29 must also be allowable for at least the same reasons as Claims 1, 13, and 23.

[12] Kanuri et al. at col. 5 ll. 43-59.

Claim 3

Claim 3 as presently amended recites:

> The network access device of claim 1, wherein the control logic is adapted to authenticate the user information in accordance with an IEEE 802.1x protocol.

The Examiner states:

> ... Kanuri et al. teaches the network access device of claim 1, wherein said control logic is adapted to authenticate said user information in accordance with an IEEE 802.1x protocol (Col 3, starting at line 36: IEEE 802.3).[13]

The Applicant respectfully disagrees. In support of the Examiner's contention, the Examiner refers to a portion of Kanuri et al. that discloses sending and receiving layer 2 data packets according to the IEEE 802.3 protocol. The IEEE 802.1X protocol enables authenticated access to IEEE 802 media, including Ethernet, Token Ring, and 802.11 wireless LANs.[14] The IEEE 802.3 protocol is described in RFC 3580, a copy of which is submitted with an Information Disclosure Statement filed herewith. The IEEE 802.3 protocol is not the same as the IEEE 802.1X protocol. Kanuri et al. does not disclose the IEEE 802.1X protocol, nor does it disclose the IEEE 802.3 protocol in the context of user authentication. For this additional reason, the 35 U.S.C. § 102 rejection of Claim 3 is unsupported by the cited art of record and the rejection must be withdrawn.

The Second 35 U.S.C. § 103 Rejection

Claims 4-5, 16, 26 and 27 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Kanuri et al. in view of Short et al., further in view of Mate et al.,[15] and further

---

[13] Office Action at p. 6.
[14] P. Congdon et al., *RFC 3580 - IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*, September 2003, at § 1.
[15] U.S. Patent No. 7,028,098 to Mate et al.

in view of Gai et al.,[16] of which no claims are independent claims.[17] This rejection is respectfully traversed.

Claims 4 and 5 depend from Claim 1. Claim 16 depends from Claim 13. Claims 26 and 27 depend from Claim 23. The arguments made above with respect to the 35 U.S.C. § 103 rejection of independent Claims 1, 13, and 23 apply here as well. The 35 U.S.C. § 103 rejection of Claims 1, 13, and 23 is unsupported by the cited art of record because each and every element as set forth in Claims 1, 13, and 23 is not taught or suggested by Kanuri et al. in view of Short et al. Accordingly, the 35 U.S.C. § 103 rejection of dependent claims 4-5, 16, and 26-27 based on Kanuri et al. in view of Short et al., further in view of Mate et al., and further in view of Gai et al. is also unsupported by the cited art of record. Thus, a *prima facie* case has not been established and the rejection must be withdrawn.

Claim 4

Claim 4 as presently amended recites:

> The network access device of claim 1, wherein the user policy identifies an access control list.

The Examiner states,

> ... Kanuri et al fails to disclose network access device wherein said user policy identifies an access control list. . However, Mate et al discloses network access device wherein said user policy identifies an access control list (Col 5, starts at line 60; Col 10, starts at line 45; policy; ACL). Furthermore, Gai et al discloses network access device wherein said user policy identifies an access control list (Fig 5; Fig 613; Par 0007-0008; 0039, 0046; ACL) Gai et al , Mate et al and Kanuri et al are analogous art because they are from the same field of endeavor of secure network communication. At the time of invention, it will be obvious to a person of ordinary skill in the art to combine the teachings of Mate et al or Gai et al with modified Short et al - Kanuri system to design an apparatus wherein user

[16] U.S. Publication No. 2004/0160903 to Gai et al.
[17] Office Action at ¶ 6.

> policy identifies an access control list to facilitate a managed packet filtering based on port or flow information.[18]

The Applicants respectfully disagree. One of ordinary skill in the art would not be motivated to combine Kanuri et al. in view of Short et al. and further in view of Gai et al. with Mate et al. because Mate et al. teaches away from the combination. Mate et al. recites:

> Policy-based routing flows are determined to have lower priority and are assigned to partition 36b. Policy based routing flows can include data classified by Access Control Lists (ACL) flows and traffic manager (TE) flows. Accordingly, MPLS flows and IP-VPN flows which have been assigned higher priority will be found in a subsequent lookup in flow TCAM 30 before ACL flows and TE flows which have been assigned a lower priority and MPLS flows or P VPN flows will subsume any matching ACL flows and TE flows in flow TCAM 30.[19]

As Mate et al. teaches assigning a lower priority to policy-based flows, which include ACL flows, one of ordinary skill in the art would not be motivated to combine Kanuri et al. in view of Short et al. with Mate et al. and Gai et al.

Furthermore, combining Kanuri et al. in view of Short et al. and further in view of Gai et al. with Mate et al. result in a complex network switch having multiple data flows with different priority levels, which would be incapable of ensuring switching of data packets at the wire rate. This would render the combination unsatisfactory for Kanuri et al.'s intended purpose of providing a network switch that is able to perform trunk-based switching of data packets at the wire rate.[20] For this additional reason, one of ordinary skill in the art would not be motivated to combine Kanuri et al. in view of Short et al. and further in view of Gai et al. with Mate et al.

---

[18] Office Action, pp. 7-8.
[19] Mate et al. at col. 5 l. 63 to col. 6 l. 5.
[20] *See* Kanuri et al., Abstract.

For these additional reasons, the 35 U.S.C. § 103 Rejection of Claim 4 is unsupported by the cited art of record and the rejection must be withdrawn.

Claim 5

Claim 5 as presently amended recites:

> The network access device of claim 1, wherein the user policy includes an access control list.

The Examiner states:

> ... Kanuri et al. fails to disclose the network access device wherein said user policy includes an access control list (Col 5, starts at line 60; Col 10, starts at line 45; policy ..including ACL).[21]

The Applicants agree that Kanuri et al. fails to disclose the network access device wherein the user policy includes an access control list.. The arguments made above with respect to Claim 4 apply here as well.

The Third 35 U.S.C. § 103 Rejection

Claims 8-10, 12, 18-22, and 30-34 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Kanuri et al. in view of Short et al. further in view of See et al.,[22] of which no claims are independent claims.[23] This rejection is respectfully traversed.

Claims 8-10 depend from Claim 1. Claims 18-22 depend from Claim 13. Claims 30-34 depend from Claim 23. The arguments made above with respect to the 35 U.S.C. § 103 rejection of independent Claims 1, 13, and 23 apply here as well. The 35 U.S.C. § 103 rejection of Claims 1, 13, and 23 is unsupported by the cited art of record because each and every element as set forth

[21] Office Action at p. 7.
[22] U.S. Patent No. 6,874,090 to See et al.
[23] Office Action at ¶ 7.

in Claims 1, 13, and 23 is taught or suggested by Kanuri et al. in view of Short et al. Accordingly, the 35 U.S.C. § 103 rejection of dependent claims 8-10, 18-22, 30-34 based on Kanuri et al. in view of Short et al. and further in view of See et al. is also unsupported by the cited art of record. Thus, a *prima facie* case has not been established and the rejection must be withdrawn.

Claim 8

Claim 8 as presently amended recites:

> The network access device of claim 1, wherein the control logic is adapted to send the user information to an authentication server and to receive an accept message from the authentication server if the user information is valid.

The Examiner states,

> ... Kanuri et al fails to teach the network access device of claim 1, wherein said control logic is adapted to send said user information to an authentication server and to receive an accept message from said authentication server if said user information is valid. However, See et al teaches control logic is adapted to send said user information to an authentication server and to receive an accept message from said authentication server if said user information is valid (Col 6, starting at line 32; Col 10, starting at line 10; claims 25-27;authentication information including VLAN identifier; user identification information). Furthermore, Short et al teaches control logic is adapted to send said user information to an authentication server and to receive an accept message from said authentication server if said user information is valid (Col 3, starts at line 10; AAA / RADIUS server authenticating user id). Short et al , See et al and Kanuri et al are analogous art because they are from the same field of endeavor of secure network communication. At the time of invention, it will be obvious to a person of ordinary skill in the art to combine the teachings of See et al with modified Short et al Kanuri system to design an apparatus further including an authentication server in order to facilitate proper VLAN authentication.[24]

The Applicants respectfully submit the Examiner's attempt to equate a VLAN identifier with the user information of Claim 8 is improper. Claim 8 requires that the control logic is

[24] Office Action, pp. 8-9.

adapted to send the user information to an authentication server and to receive an accept message from the authentication server if the user information is valid. Claim 1 from which Claim 8 depends requires that the user information is provided by a user of the user device. The VLAN identifier of See et al. cannot be the to be provided by a user of the device, nor can it be the to be user information. For this additional reason, the 35 U.S.C. § 103 Rejection of Claim 8 is unsupported by the cited art of record and the rejection must be withdrawn.

The Fourth 35 U.S.C. § 103 Rejection

Claims 35-37 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Kanuri et al. in view of Short et al., further in view of See et al., and further in view of Volpano,[25] of which no claims are independent claims.[26] This rejection is respectfully traversed.

Claim 35

Claim 35 as presently amended recites:

> The network access device of claim 2 wherein the control logic is further configured to:
> if authentication of the MAC address indicates the MAC address is invalid,
> drop packets from the user device; or
> disable the port;
> if authentication of the user information indicates the user information is invalid,
> block all traffic on the port except for packets related to a user authentication protocol;
> if authentication of user information indicates the user information is valid,
> determine whether the user is associated with a VLAN supported by the network access device;
> if the user is not associated with the VLAN,
> assign the port to a port default VLAN; and
> block all traffic on the port except for packets related to the user authentication protocol; and
> if the user is associated with the VLAN,
> assign the port to the VLAN associated with the user; and

[25] U.S. Patent No. 7,188,364 to Volpano.
[26] Office Action at ¶ 8.

forward packets from the user device.

The Examiner states,

they are rejected applying as above rejecting claims 1, 14 and 24. Furthermore, Kanuri et al discloses network access device/ method/ apparatus wherein said control logic is further configured to:
if authentication of said MAC address indicates said MAC address is invalid (Fig 3, step 70106; Col 5, lines 43-60; authenticating MAC address); or
disable said port (Col 5, starts at line 40; disabling port).
... Kanuri et al fails to disclose if authentication of said user information indicates said user information is invalid, block all traffic on said port except for packets related to a user authentication protocol; if authentication of user information indicates said user information is valid, determine whether said user is associated with a VLAN supported by said network access device;
if said user is not associated with said VLAN, assign said port to a port default VLAN; andblock all traffic on said port except for packets related to said user authentication protocol; and
if said user is associated with said VLAN, assign said port to said VLAN associated with saiduser; and forward packets from said user device.
However, Short et al discloses if authentication of user information indicates said user information is valid, determine whether said user is associated with a VLAN supported by said network access device (Col 3, starts at line 12; packet transmission; VLAN, user Id authenticating); and if said user is associated with said VLAN, assign said port to said VLAN associated with said user; and forward packets from said user device (Col 3, starts at line 12). Furthermore, See et al discloses dropping packets if MAC address is not valid, if authentication of user information indicates said user information is valid, determine whether said user is associated with a VLAN supported by said network access device ; and if said user is associated with said VLAN, assign said port to said VLAN associated with said user; and forward packets from said user device (Col 3, starts at line 10; authenticating user identification information in VLAN; packet transmission). Modified Short et al-Kanuri system fails to disclose if authentication of said user information indicates said user information is invalid, block all traffic on said port except for packets related to a user authentication protocol; and if said user is not associated with said VLAN, assign said port to a port default VLAN; and block all traffic on said port except for packets related to said user authentication protocol;
However, Volpano discloses if authentication of said user information indicates said user information is invalid, block all traffic on said port except for packets related to a user authentication protocol; and if said user is not associated with said VLAN, assign said port to a port default VLAN; and block all traffic on said port except for packets related to said user authentication protocol (Col 5, starting at line 30; control frames; EAPOL). Volpano and Kanuri et al are analogous art because they are from the same field of endeavor of VLAN utilizing bridges/ switches. At the time of invention, it will be obvious to a person of ordinary skill in the art to combine the teachings of Volpano with modified See at al Short et al - Kanuri et al apparatus/ method/ system to design an apparatus further adapted to

> drop/ filter packets by authenticating utilizing an authentication server, authentication protocol message containing VLAN identifier in order to provide a proper VLAN packet filtering.[27]

The Applicants respectfully disagree. The arguments regarding the 35 U.S.C. § 103 rejection of Claims 1-3, 6-7, 11, 13-15, 17, 23-25, 28-29, and 44-46 based on Kanuri et al. in view of Short et al., and the 35 U.S.C. § 103 rejection of Claims 8-10, 18-22, and 30-34 based on Kanuri et al. in view of Short et al. and further in view of See et al. apply here as well. For this reason, the 35 U.S.C. § 103 Rejection of Claims 35-37 is unsupported by the cited art of record and the rejection must be withdrawn.

The Fifth 35 U.S.C. § 103 Rejection

Claims 38-43 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Kanuri et al. in view of Short et al., further in view of See et al., and further in view of Volpano, of which Claims 38, 40, and 42 are independent claims.[28] This rejection is respectfully traversed.

Claim 38

Claim 38 as presently amended recites:

> An apparatus for providing network security, comprising:
> a plurality of input ports;
> a switching fabric for routing data received on the plurality of input ports to at least one output port; and
> control logic adapted to:
> authenticate a physical address of a user device coupled to one of the plurality of input ports;
> drop packets from the user device if the physical address is invalid;
> authenticate user information provided by a user of the user device only if the physical address is valid;

[27] Office Action, pp. 10-12.
[28] Office Action at ¶ 9.

if authentication of the user information indicates the user information is invalid, block all traffic on the one of the plurality of input ports except for packets related to a user authentication protocol;
if authentication of user information indicates the user information is valid, determine whether the user is associated with a VLAN supported by the apparatus by receiving a message from an authentication server, wherein the message comprises a VLAN identifier (ID) associated with the user information;
if the user is not associated with the VLAN,
assign the one of the plurality of input ports to a port default VLAN; and
block all traffic on the one of the plurality of input ports except for packets related to the user authentication protocol; and
if the user is associated with the VLAN,
assign the one of the plurality of ports to the VLAN associated with the user; and
restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information.

The Examiner states,

... Kanuri et al teaches an apparatus/ method/ system for providing network security, comprising:
A data communication network (Col 3, starts at line 26; network packets);
A network access device coupled to said data communication network (Col 3, starts at line26; switch enabling communication);
a plurality of input ports (Fig l, 12.22; Col 3, lines 25-67; multiport switch);
a switching fabric for routing data received on said plurality of input ports to at least one output port (Fig 1.28; Col 3, lines 25-67; switch fabric; Col 4, lines 7-52; layer 2 switch); and control logic adapted to:
authenticate a physical address of a user device coupled to one of said plurality of input ports (Col 3, line 28 to Col 5, line 65: the switch; MAC module; switching (rules) logic; matching MAC addresses);
authenticate user information provided by a user of said user device only if said physical address is valid (Col 3, line 54 to Col 4, line 34; Col 5, lines 10-65; user or network nodes' attributes/ policies/ information; user defined policies/ attributes; authenticating VLAN field/ index/ information, and MAC addresses specific to user/ network node/ data frame);
if authentication of user information indicates said user information is valid, determine whether said user is associated with a VLAN supported by said apparatus, wherein said message comprises a VLAN identifier (ID)
associated with said user information (Col 5, lines 1-65; determining/ matching VLAN index/ information);
if said user is associated with said VLAN, assign said one of said plurality of ports to said VLAN associated with said user (Col 5, lines 1-20; Col 6, lines 1-40; switching logic assigning/ selecting ports);

if said user is not associated with said VLAN, assign said one of said plurality of input ports to a port default VLAN (Col 5, lines 1-20; Col 6, lines 1-40; switching logic assigning/ selecting ports); and
restrict access to said one of said plurality of input ports in accordance with a user policy associated with said user information (Fig 2:40; associated port, MAC and VLAN information; Fig 3, step 70-106; Col 5, lines 43-60; if in step 74 the switching rules logic determined a match between MAC...VLAN index .... (then) checks in step 76 whether port ..; the examiner interprets switching "rules" logic as policy; port filtering).
In the case, obviousness regarding authenticating user provided authentication information, and MAC is not found to be supportive, the examiner notes, Short et al discloses network security/ access device authenticating user provided authentication information, and MAC (Fig 2; Col 4, starts at line 12; authentication; user id; MAC). Kanuri et al fails to disclose expressly drop packets from said user device if said physical address is invalid;
if authentication of said user information indicates said user information is invalid, block alltraffic on said one of said plurality of input ports except for packets related to a user authentication protocol; receiving a message from an authentication server, wherein said message comprises a VLAN identifier (ID) associated with said user information;
if said user is not associated with said VLAN, block all traffic on said one of said plurality of input ports except for packets related to said user authentication protocol.
However, See et al discloses drop packets from said user device if said physical address is invalid (Col 6, starting at line32; filtering/ dropping packets based on MAC/ VLAN identifier);
receiving a message from an authentication server, wherein said message comprises a VLAN identifier (ID) associated with said user information (Col 6, starting at line 32; Col 10, starting at line 10; claims 25-27; authentication information including VLAN identifier; user identification information);
Modified See at al - Short et al- Kanuri et al apparatus/ method/ system fails to disclose if authentication of said user information indicates said user information is invalid, block all traffic on said one of said plurality of input ports except for packets related to a user authentication protocol.
if said user is not associated with said ULAN, block all traffic on said one of said plurality of input ports except for packets related to said user authentication protocol.
However; Volpano discloses if authentication of said user information indicates said user information is invalid, block all traffic on said one of said plurality of input ports except for packets related to a user authentication protocol (Col 5, starting at line 30; control frames; EAPOL);
if said user is not associated with said VLAN, block all traffic on said one of said plurality of input ports except for packets related to said user authentication protocol (Col 5, starting at line 30; control frames; EAPOL). Volpano and Kanuri et al are analogous art because they are from the same field of endeavor of VLAN utilizing bridges/ switches. At the time of invention, it will be obvious to a person of ordinary skill in the art to combine the teachings of modified See at al - Short et

> al-Kanuri et al apparatus/ method/ system with Volcano to design an apparatus further adapted to drop/ filter packets by authenticating utilizing an authentication server, authentication protocol message containing VLAN identifier in order to provide a proper VLAN packet filtering.[29]

The Applicants respectfully disagree. The arguments regarding the 35 U.S.C. § 103 rejection of Claims 1-3, 6-7, 11, 13-15, 17, 23-25, 28-29, and 44-46 based on Kanuri et al. in view of Short et al., and the 35 U.S.C. § 103 rejection of Claims 8-10, 18-22, and 30-34 based on Kanuri et al. in view of Short et al. and further in view of See et al. apply here as well. For this reason, the 35 U.S.C. § 103 Rejection of Claims 38, 40, and 42 is unsupported by the cited art of record and the rejection must be withdrawn.

Claims 39, 41, and 43

Claims 39, 41, and 43 depend from Claims 38, 40, and 42, respectively. Claims 38, 40, and 42 being allowable. Claims 39, 41, and 43 must also be allowable for at least the same reasons as for Claims 38, 40, and 42, respectively.

In view of the foregoing, it is respectfully asserted that the claims are now in condition for allowance.

Conclusion

It is believed that this Amendment places the above-identified patent application into condition for allowance. Early favorable consideration of this Amendment is earnestly solicited.

[29] Office Action, pp. 12-16.

If, in the opinion of the Examiner, an interview would expedite the prosecution of this application, the Examiner is invited to call the undersigned attorney at the number indicated below.

The Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Please charge any additional required fee or credit any overpayment not otherwise paid or credited to our deposit account No. 50-1698.

Respectfully submitted,

THELEN REID BROWN
RAYSMAN & STEINER LLP

Dated: April 30, 2008

John P. Schaub
Reg. No. 42,125

THELEN REID BROWN RAYSMAN & STEINER LLP
P.O. Box 640640
San Jose, CA 95164-0640
Tel. (408) 292-5800
Fax. (408) 287-8040

Atty. Docket No.: 034300-364

Applicant/Attorney Interview Summary

Application No.: 10/654,417 **First Named Applicant:** Philip Kwan

Examiner: Shanto Abedin **Art Unit:** 2136 **Status of Application:** Pending

Participants: (1) John P. Schaub **(2)** Shanto Abedin

(3)_____ **(4)**_____

Date of Interview: 4/2/2008 **Time:** 3:00 PM (EST)

Type of Interview:
(a) [X] Telephonic **(b) [ ] Personal** **(c) [ ] Video Conference**

Exhibit Shown or Demonstrated: [ ] YES [X] NO
If yes, provide brief description:

Issues Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
Rej.	Claim 1	Kanuri et al., Short et al.	[X]	[ ]	[X]

[ ] Continuation Sheet Attached [ ] Copy of Amendment attached

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments:

The 103 rejection of Claim 1, based on Kanuri et al. in view of Short et al. was discussed. No agreement was reached.

Note: The MPEP, section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the Examiner was reached at the interview.

In every instance where reconsideration is requested in view of an interview with an Examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed be the Applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

_____
(Applicant/Applicant's Representative Signature)